Journal of
CRYPTOLOGY
Volume 9, 1996

The Journal of the International Association for Cryptologic Research

Editor-in-Chief: Gilles Brassard

Mail:
Département IRO
Université de Montréal
C.P. 6128, succursale centre-ville
Montréal, Québec
Canada H3C 3J7

brassard@iro.umontreal.ca
Tel: 1 514 343-6807
Fax: 1 514 343-5834

Courier:
Université de Montréal
Pavillon André-Aisenstadt
Département IRO, local 3349
2900 Edouard-Montpetit
Montréal, Québec
Canada H3T 1J8

Editorial Board

Thomas A. Berson
Anagram Laboratories
764 Forest Avenue
Palo Alto, CA 94301, USA
berson@anagram.com

Ernest F. Brickell
9308 Avenida de la Luna, NE
Albuquerque, NM 87111, USA
brickell@btec.com

Johannes Buchmann
Technische Hochschule Darmstadt
FB Informatik
Alexanderstrasse 10
D-64283 Darmstadt, Germany
buchmann@cdc.informatic.th-darmstadt.de

David Chaum
Cryptography Group
Centre for Mathematics and Computer Science
Kruislaan 413
1098 SJ Amsterdam
The Netherlands

Don Coppersmith
IBM Research
Thomas J. Watson Research Center
Yorktown Heights
NY 10598, USA
COPPER@watson.ibm.com

Ivan B. Damgård
Matematisk Institut
Aarhus University
Ny Munkegade 116
DK-8000 Aarhus C, Denmark
ivan@daimi.aau.dk

Joan Feigenbaum
Room 2C-473
AT&T Bell Laboratories
600 Mountain Avenue
Murray Hill, NJ 07974-0636, USA
jf@research.att.com

Oded Goldreich
Department of Applied Mathematics and Computer Science
Weizmann Institute of Science
Rehovot 76100, Israel
oded@wisdom.weizmann.ac.il

David Kahn
120 Wooleys Lane
Great Neck, NY 11023, USA

James L. Massey
Digital System Engineering
ETH Zentrum
CH-8092 Zürich, Switzerland
massey@isi.ee.ethz.ch

Ueli M. Maurer
Institute for Theoretical Computer Science
ETH Zürich
CH-8092 Zürich, Switzerland
maurer@inf.ethz.ch

Andrew M. Odlyzko
Room 2C-355
AT&T Bell Laboratories
600 Mountain Avenue
Murray Hill, NJ 07974-0636, USA
amo@research.att.com

Steven Rudich
Carnegie Mellon University
5000 Forbes Avenue
School of Computer Science
Pittsburgh, PA 15213-3890, USA
rudich@theory.cs.cmu.edu

Adi Shamir
Dr. Shamir is currently on sabbatical leave

Othmar Staffelbach
UG FU Sektion Kryptologie
Hofweg 11
CH-3003 Bern, Switzerland
staffel@inf.ethz.ch

Jacques Stern
Département de Mathématiques et d'Informatique
École Normale Supérieure
45 rue d'Ulm
75230 Paris 05, France
stern@dmi.ens.fr

Douglas R. Stinson
Computer Science and Engineering Department
115 Ferguson Hall
University of Nebraska
Lincoln, NE 68588-0115, USA
stinson@bibd.unl.edu

Andrew C.-C. Yao
Department of Computer Science
Princeton University
Princeton, NJ 08544, USA
yao@princeton.edu

Aims and Scope

Journal of Cryptology provides a forum for original results in all areas of modern information security. Both cryptography and cryptanalysis are covered, including information theoretic and complexity theoretic perspectives as well as implementation, application, and standards issues. Illustrative topics include public key and conventional algorithms and their implementations, cryptanalytic attacks, pseudo-random sequences, computational number theory, cryptographic protocols, untraceability, privacy, authentication, key management, and quantum cryptography. In addition to full-length technical, survey, and historical articles, short notes are acceptable.

The exclusive copyright for all languages and countries, including the right for photomechanical and any other reproductions, also in microform, is transferred to the publisher.
The use of registered names, trademarks, etc., in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Printed in the United States of America
© 1996 International Association for Cryptologic Research

Index to Volume 9

BELLARE, M.: Certifying Permutations: Noninteractive Zero-Knowledge Based on Any Trapdoor Permutation 149
BEN-AROYA, I.: Differential Cryptanalysis of Lucifer 21
BIHAM, E.: *see* BEN-AROYA, I. 21
CRÉPEAU, C.: Guest Editor's Introduction 127
DE SANTIS, A.: The Power of Preprocessing in Zero-Knowledge Proofs of Knowledge 129
EVEN, S.: On-Line/Off-Line Digital Signatures 35
FISCHER, M. J.: A Secure Protocol for the Oblivious Transfer (Extended Abstract) 191
FISCHER, M. J.: Bounds on Secret Key Exchange Using a Random Deal of Cards 71
FRANKLIN, M.: Joint Encryption and Message-Efficient Secure Computation 217
GOLDREICH, O.: How To Construct Constant-Round Zero-Knowledge Proof Systems for NP 167
GOLDREICH, O.: *see* EVEN, S. 35
GOLIĆ, J. DJ.: Correlation Properties of a General Binary Combiner with Memory 111
HABER, S.: *see* FRANKLIN, M. 217
HEMASPAANDRA, L. A.: *see* YENJO HEN 251
HEYS, H. M.: Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis 1
IMPAGLIAZZO, R.: Efficient Cryptographic Schemes Provably as Secure as Subset Sum 199
JACKSON, W.-A.: Ideal Secret Sharing Schemes with Multiple Secrets 233
KAHAN, A.: *see* GOLDREICH, O. 167
MARTIN, K. M.: *see* JACKSON, W.-A. 233
MASAFUMI HOSHI: *see* TOSHIYA ITOH 101
MICALI, S.: *see* EVEN, S. 35
MICALI, S.: *see* FISCHER, M. J. 191
NAOR, M.: *see* IMPAGLIAZZO, R. 199
O'KEEFE, C. M.: *see* JACKSON, W.-A. 233
PERSIANO, G.: *see* DE SANTIS, A. 129
RACKOFF, C.: *see* FISCHER, M. J. 191
SHIGEO TSUJII: *see* TOSHIYA ITOH 101
TAVARES, S. E.: *see* HEYS, H. M. 1
TOSHIYA ITOH: A Low Communication Competitive Interactive Proof System for Promised Quadratic Residuosity 101
WRIGHT, R. N.: *see* FISCHER, M. J. 71
YENJO HAN: Pseudorandom Generators and the Frequency of Simplicity 251
YUNG, M.: *see* BELLARE, M. 149